



PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
G06F 9/06

A1

(11) 国際公開番号

WO00/42498

(43) 国際公開日

2000年7月20日(20.07.00)

(21) 国際出願番号 PCT/JP99/00084

(22) 国際出願日 1999年1月13日(13.01.99)

(71) 出願人 (米国を除くすべての指定国について)

株式会社 日立製作所(HITACHI, LTD.)(JP/JP)

〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ)

鍛 忠司(KAJI, Tadashi)(JP/JP)

洲崎誠一(SUSAKI, Seiichi)(JP/JP)

〒215-0013 神奈川県川崎市麻生区王禅寺1099番地

株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP)

赤尾杉隆(AKAOSUGI, Takashi)(JP/JP)

〒244-8555 神奈川県横浜市戸塚区戸塚町5030番地

株式会社 日立製作所 ソフトウェア事業部内 Kanagawa, (JP)

(74) 代理人

弁理士 小川勝男(OGAWA, Katsuo)

〒100-8220 東京都千代田区丸の内一丁目5番1号

株式会社 日立製作所内 Tokyo, (JP)

(81) 指定国 AU, CA, IL, JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類

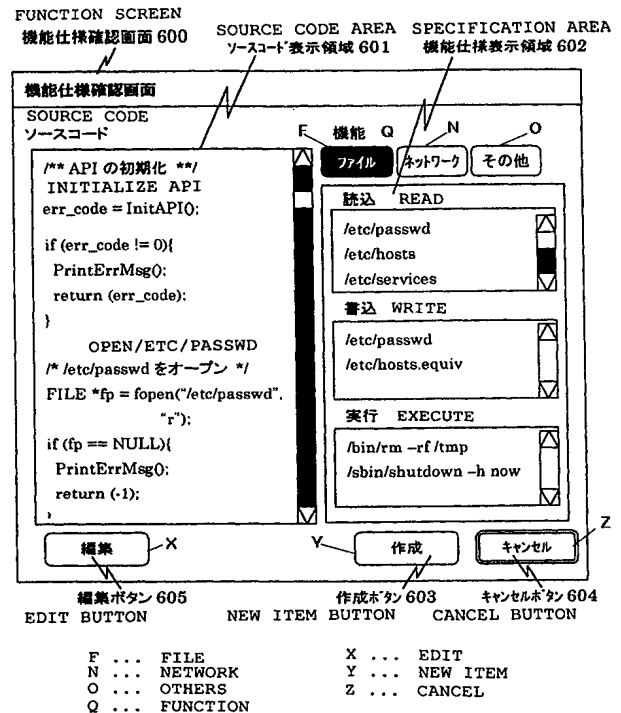
国際調査報告書

(54)Title: METHOD AND SYSTEM FOR EXECUTING MOBILE CODE

(54)発明の名称 モバイルコードの実行方法およびそのシステム

(57) Abstract

Means for deciding whether to execute a mobile code depending on the functions of the mobile code. When a mobile-code receiving section at a user terminal receives data including a mobile code from a distributor server, a signature attached to the mobile code is checked. When the signature is successfully verified, a function confirmation section confirms the specification that describes the functions of the mobile code. If the function confirmation section decides to permit the execution of the mobile code, a mobile code execution means executes the mobile code.



(57)要約

モバイルコードが持っている機能に基づいて、当該モバイルコードを実行するか否かを決定する手段を提供することを目的とする。

ユーザー端末において、モバイルコード受信処理部が配布サーバからモバイルコードを含む配布データを受信した場合、まず、前記モバイルコードに付加されている署名を検証する。署名の検証に成功した場合、次に、前記機能確認処理部が当該モバイルコードの機能を記述した機能仕様を確認する。前記機能仕様確認処理部が当該モバイルコードの実行を許可すると判断した場合に、モバイルコード実行手段が前記モバイルコードを実行する。

PCTに基づいて公開される国際出願のパフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサオ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明 細 書

モバイルコードの実行方法およびそのシステム

技術分野

本発明は、サーバからネットワークを介してユーザー端末にダウンロードされ、自動的に実行されるモバイルコードのセキュリティに関する。

背景技術

World Wide Web (WWW)の表現力や利便性を大幅に高める手段として、モバイルコードが広く用いられてきている。モバイルコードは、WWWサーバ上に置いておき、ユーザー端末を利用するユーザーがBrowserプログラムを用いて、当該ページにアクセスしたときにダウンロードされ、自動的に実行される、というプログラムである。

しかし、その一方で、ユーザー端末上のリソース(ファイルや周辺機器など)に勝手にアクセスし、情報を盗んだり、障害を引き起こすといった、不正な処理を行うモバイルコードが問題となってきている。

そのため、モバイルコードを利用するシステムには、モバイルコードの実行に対して、以下のようなセキュリティ機能を設けているものがある。

(1) モバイルコードには、ユーザー端末上のリソースへのアクセスを基本的に認めない。

(2) モバイルコードは、そのモバイルコードが保管されていたサーバとの間でしか通信することができない。

このようなセキュリティ機能は、不正なモバイルコードからシステムを守るために考えだされたものである。

しかし、その一方で、このような規制がモバイルコードの利便性を損なうものであることも明らかである。そのため、モバイルコードが、そのモバイルコードの作成者の署名(電子的な署名でデジタル署名と呼ばれる)が付加された、いわゆる署名付きコードであり、かつ、その作成者のモバイルコードならば信用するとユーザー端末を利用するユーザーが認めた場合には、上記モバイルコードに対する制限は適用されないように機能拡張されてきている。例えば、特開平10-83310号公報には、このような署名付きコードを利用するシステムの一例が示されている。また、上記デジタル署名技術については、例えば「SECURE ELECTRONIC COMMERCE」(PRENTICE HALL、1997) pp. 111-116に記載されている。

ローカルファイルにアクセスする署名付きコードを、ネットワークを介してサーバからダウンロードした場合の、当該ユーザー端末での処理手順例を第19図を参照して簡単に説明すると、以下のようである。

ユーザー端末を利用するユーザーが、Browserプログラムを用いて署名付きコードをサーバからダウンロードすると(ステップ1901)、まず、署名付きコードに付加されたデジタル署名を検証し、モバイルコードの完全性(改ざんされていないこと)を確認する(ステップ1902)。完全性が確認された場合には、次に、その署名の署名者が、すでにローカルファイルへのアクセスを許可されている署名者であるかどうかを確認し(ステップ1903)、アクセスが許可された署名者であった場合には、署名付きコードがローカルファイルにアクセスして、あらかじめプログラミングされた処理を実行する(ステップ1905)。

また、ステップ1903において、アクセスが許可されていない署名者であった場合、ユーザー端末を利用しているユーザーに対して、当該署名者が作成した署名付きコードにローカルファイルへのアクセス許可を与

3

えるかどうかを選択させる(ステップ1904)。許可が与えられた場合には、署名付きコードがローカルファイルにアクセスしてあらかじめプログラミングされた処理を実行する(ステップ1905)。

5 ステップ1902において完全性が確認できなかった場合、およびステップ1904においてアクセスの許可が与えられなかった場合には、ユーザー端末を利用しているユーザーにその旨を通知し(ステップ1906)、処理を終了する。

10 上述の署名付きコードのセキュリティ機能は、モバイルコードの署名者によってモバイルコードの実行を許可するか否かを判断するものであり、当該モバイルコードがどのような機能を持っているのかは、実行してみるまでわからない。そのため、ユーザーは、当該モバイルコードを実行してみるまでは、実行してよいか否かの十分な情報を得ることができない。そして、ユーザーが署名者を信頼すると判断した場合には、署名付きコードが不正な処理を行うモバイルコードであっても、実行され
15 てしまうという問題がある。

特開平10-83310号公報には、コードと共に当該コードが要求するリソースの一覧(ACL)を配布し、実行時に当該ACLにしたがってリソースを割当てるという方法が開示されている。コードと共にACLを配布することによって、コードがどのリソースにアクセスするのかを実行前に知る
20 ことはできるが、そのリソースをどのように使用するのか、すなわち、コードがどのような機能を持っているのかはわからない。

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、モバイルコードが持っている機能に基づいて、当該モバイルコードを実行するか否かを決定することができる、モバイルコードの構成と当該モ
25 バイルコードの実行方法と、それを利用したモバイルコードシステム、さらには、そこに用いるソースコード作成端末、機能検証サーバ、モバ

イルコード配布サーバ、ユーザー端末、およびそれらを実現するプログラムを提供することにある。

発明の開示

- 5 上記目的を達成するため、本発明のモバイルコードには、当該モバイルコードの持つ機能を記述した機能仕様、または当該機能仕様に対応づけられた識別子が添付されていることを特徴とする。

- さらに、本発明のモバイルコードの実行方法は、前記モバイルコードを実行する前に、それが持つ機能を確認し、実行するか否かを判断する
10 ステップを設けたことを特徴とする。

- すなわち、本発明のモバイルコードの実行方法は、モバイルコードを取得する、モバイルコード取得ステップと、前記モバイルコード取得ステップによって取得された前記モバイルコードに付加されている電子的な署名を検証する、署名検証ステップと、前記署名検証ステップによっ
15 て、当該モバイルコードの署名の検証に成功した(検証結果が合格であった)場合に、当該モバイルコードの持つ機能を記述した機能仕様を取得する、機能仕様取得ステップと、前記機能仕様取得ステップで取得した前記機能仕様によって、前記モバイルコードの持つ機能を確認し、当該モバイルコードを実行するか否かを判断する、機能確認ステップと、
20 前記機能確認ステップにおいて、前記モバイルコードは実行を許可されると判断された場合に、当該モバイルコードを実行する、モバイルコード実行ステップと、を備えている。

- また、本発明のモバイルコードシステムは、モバイルコードのソースコードを作成するソースコード作成端末と、ソースコードの機能を検証
25 する機能検証サーバと、モバイルコードを配布するモバイルコード配布サーバと、モバイルコードを実行するユーザー端末と、からなるモバイ

ルコードシステムであって、

前記ソースコード作成端末は、モバイルコードのソースコードを作成するソースコード作成手段と、前記モバイルコードのソースコードを前記機能検証サーバに送信するソースコード送信手段と、を備え、

- 5 前記機能検証サーバは、送信された前記モバイルコードのソースコードから当該モバイルコードの持つ機能を記述した機能仕様を作成し、当該モバイルコードが不正な処理を行うものでないかを検証する機能検証手段と、前記機能検証手段が前記モバイルコードは不正な処理を行うものではないと判断した場合に、前記ソースコードから前記モバイルコードを作成するモバイルコード作成手段と、前記配布サーバに対して、前記モバイルコード作成手段によって作成された、モバイルコードの登録を要求する登録要求手段と、を備え、
- 10

- 前記モバイルコード配布サーバは、前記登録を要求された前記モバイルコードを格納し、保管するモバイルコード保管手段と、前記ユーザー
- 15 端末から配送を要求された、前記モバイルコード保管手段が保管している前記モバイルコードを前記ユーザー端末に送信するモバイルコード送信手段と、を備え、

- 前記ユーザー端末は、前記モバイルコード配布サーバに対して、モバイルコードの配送を要求する配送要求送信手段と、配送されたモバイル
- 20 コードに付加されている電子的な署名を検証する署名検証手段と、前記署名検証手段が署名の検証に成功した場合、前記検証サーバの機能検査手段が作成した前記機能仕様を取得し、当該機能仕様によって前記モバイルコードの持つ機能を確認し、当該モバイルコードの実行を許可するか否かを判断する機能確認手段と、前記機能確認手段が前記モバイルコードの実行を許可すると判断した場合に、前記モバイルコードを実行する
- 25 モバイルコード実行手段と、を備えている。

さらに、本発明のモバイルコードシステムでは、前記機能確認手段は、前記機能仕様と同じ機能仕様が、ユーザー端末に保管されている機能仕様管理ファイルに登録されているか、または、前記機能仕様をユーザーに提示し、ユーザーが当該機能を持つモバイルコードの実行を許可すると判断した場合に、当該モバイルコードの実行を許可すると判断する。

したがって、本発明では、モバイルコードをダウンロードしたユーザー端末は、当該モバイルコードを実行する前に、当該モバイルコードの持つ機能を記述した機能仕様を確認する処理を行う。そして、前記機能仕様が、予め実行を許可されたものであるか、または、ユーザーが当該機能仕様を持つモバイルコードの実行を許可すると判断した場合にのみ、前記モバイルコードが実行されるようにしている。

このため、本発明によれば、モバイルコードが持っている機能に基づいて、当該モバイルコードを実行するか否かを決定することができる。

なお、本発明はモバイルコードに限るものではなく、ユーザー端末の記憶装置に格納されているような、一般のプログラムコードを実行する場合にも適用可能である。

図面の簡単な説明

第1図は、本発明の一実施形態が適用されたモバイルコード配布システムの機器概略構成、及びハードウェア構成を示す図であり、第2図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの機能検証依頼処理に関係した、作成端末および検証サーバの機能ブロック構成を示す図であり、第3図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの機能検証処理および登録処理に係る、検証サーバおよび配布サーバの機能ブロック構成を示す図であり、第4図は、本発明の一実施形態が適用されたシステムにおいて、モバイ

ルコードの実行処理に関係する、配布サーバおよびユーザー端末の機能ブロック構成を示す図であり、第5図は、第3図において、検証サーバが作成する機能仕様の一例を示す図であり、第6図は、第3図において、検証サーバが検証者に対して表示する機能仕様確認画面の画面の一例であり、第7図は、第3図において、検証サーバが検証者に対して表示する機能仕様編集画面の画面の一例であり、第8図は、第4図において、ユーザー端末がユーザーに対して表示する実行確認画面の一例であり、第9図は、第4図に示す機能仕様管理ファイルに格納されている情報の一例を説明するための図であり、第10図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの機能検証依頼処理に関係する、作成端末の動作を説明するためのフロー図であり、第11図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの機能検証依頼処理に関係する、検証サーバの動作を説明するためのフロー図であり、第12図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの機能検証処理に関係する、検証サーバの動作を説明するためのフロー図であり、第13図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの登録に関係する、配布サーバの動作を説明するためのフロー図であり、第14図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの実行に関係する、配布サーバの動作を説明するためのフロー図であり、第15図は、本発明の一実施形態が適用されたシステムにおいて、モバイルコードの実行に関係する、ユーザー端末の動作を説明するためのフロー図であり、第16図は、本発明の他の実施形態が適用されたシステムにおいて、モバイルコードの実行に関係する、検証サーバ、配布サーバおよびユーザー端末の機能ブロック構成を示す図であり、第17図は、本発明の他の実施形態が適用されたシステムにおいて、モバイルコードの実行に関係する、ユーザー端末

の動作を説明するためのフロー図であり、第18図は、本発明の他の実施形態が適用されたシステムにおいて、モバイルコードの実行に関する、検証サーバの動作を説明するためのフロー図であり、第19図は、従来のモバイルコードにおけるセキュリティ機能を説明するためのフロー図であり、第20図は、第4図において、ユーザー端末がユーザーに対して表示する実行確認画面の一例である。

発明を実施するための最良の形態

以下、図面を用いて、本発明の実施形態について説明する。なお、これにより本発明が限定されるものではない。

第1図は、本発明の一実施形態が適用されたモバイルコードシステムの機器概略構成、及びハードウェア構成を示す図である。

本実施形態のシステムは、第1図に示すように、モバイルコードのソースコードを作成する、ソースコード作成端末110(以下、単に作成端末110とも称する)と、ソースコードの機能を検証し、当該ソースコードからモバイルコードを作成する、機能検証サーバ120(以下、単に検証サーバ120とも称する)と、モバイルコードを登録し、配布する、モバイルコード配布サーバ130(以下、単に配布サーバ130とも称する)と、モバイルコードを実行する、ユーザー端末140と、が、それぞれ、コンピュータ上に構成されて、LANなどの通信網100を介して、互いに接続されて構成されている。

なお、第1図において複数の、作成端末110、検証サーバ120、配布サーバ130、またはユーザー端末140が接続されていてもよい。

前記作成端末110、検証サーバ120、配布サーバ130、とユーザー端末140を構成するコンピュータは、第1図に示すように、通信網インタフェースと、表示装置と、入力装置と、記憶装置と、中央処理装置(CPU)と、

一時記憶装置(メモリ)とが、バスによって互いに接続されて構成されている。通信網インターフェース111、121、131、141は、通信網100を介したデータの送受信を行うためのインタフェース装置である。表示装置112、122、132、142は、上記各端末、サーバを使用する使用者へのメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。入力装置113、123、133、143は、前記使用者がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。記憶装置114、124、134、144は、プログラムやデータなど種々の情報を永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

CPU115、125、135、145は、各部を統括的に制御したり、様々な演算処理を行ったりする。メモリ116、126、136、146には、オペレーティングシステム(以下、単にOSとも称する)116a、126a、136a、146aや、CPUが上記各端末、サーバの機能を実現するために必要なプログラム、データなどが格納される。

ここで、OS116aは、ユーザー端末110全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

コード作成プログラム116bは、前記作成端末110の使用者(以下、単に作成者とも称する)の指示にしたがって、モバイルコード146cのソースコード(以下、単にソースコードとも称する)を作成し、記憶装置114に格納するためのプログラムである。検証依頼プログラム116cは、前記作成者の指示にしたがって、記憶装置114に格納されている、前記ソースコードを検証サーバ120に送信するためのプログラムである。

コード検証プログラム126bは、作成端末110から前記ソースコードを受信し、当該ソースコードの機能を検証し、当該ソースコードから、モ

バイルコード146cや、その機能仕様を作成し、それらを前記配布サーバ130に登録するためのプログラムである。

コード配布プログラム136bは、検証サーバ120からモバイルコード146cを受信した場合に、前記モバイルコード146cを記憶装置134に格納し、また、ユーザー端末140からBrowserプログラム146bによるアクセスがあった場合に、記憶装置134に格納されているモバイルコード146cを、必要に応じてマルチメディアデータなどを添付して、送信するプログラムである。

また、Browserプログラム146bは、ユーザー端末140が配布サーバ130と通信し、配布データ、すなわちモバイルコード146cと必要に応じて添付される種々のデータ(たとえば、音声、画像、動画などのマルチメディアデータを含むHTMLファイル)からなるデータ、をダウンロードし、モバイルコード146cの機能を確認し、当該モバイルコード146cを実行するためのプログラムである。なお、これらの添付される種々のデータは、Browserプログラム146bが当該モバイルコード146cを実行する際に必要とされるものである。

モバイルコード146cは、ユーザー端末140の各種リソースにアクセスを行い、計算処理を行うプログラムである。

なお、本実施形態では、モバイルコード146cには、当該モバイルコード146cの実行コード以外に、当該モバイルコード146cの機能仕様、前記検証者の署名(本実施形態では署名を検証するために必要なデータをまとめて署名と記述する)や、モバイルコード自身が使用するデータやファイルが含まれており、モバイルコード146c自体の完全性の確認(改ざんされているかどうかの確認)や機能の確認に利用可能である。

次に、本実施形態における各プログラムの機能ブロック構成とその動作について説明する。以下の説明において、各機能ブロックは、上記

CPUがOSを介して、あるいは直接に、プログラムを実行することによって、実現されるものである。

ただし、前記作成者が作成端末110で前記ソースコードを作成する場合の、機能ブロック構成、および動作については、従来のモバイルコードシステムにおいて前記ソースコードを作成する場合と同じであり、その詳細な説明は省略する。なお、前記作成者が作成した前記ソースコードは、記憶装置114のソースコードファイル202に格納される。

まず、作成端末110が、モバイルコード146cの機能検証を、検証サーバ120に依頼する場合の、作成端末110および検証サーバ120の機能ブロック構成、および動作について、第2図、第10図、第11図を参照して説明する。

第2図は、作成端末110が、モバイルコード146cの機能検証を、検証サーバ120に依頼する場合の、作成端末110および検証サーバ120の機能ブロック構成を示す図である。まず、作成端末110の機能ブロック構成について説明する。

作成端末110は、第2図に示すように、入力装置113を介して、前記作成者の指示を受け付ける入力部204と、前記入力部204に入力されたデータなどを、表示装置112に表示させる表示部203と、前記入力装置113に入力された前記作成者の指示にしたがい、検証サーバ120に対して、通信網100を介して、記憶装置114のソースコードファイル202に格納された、前記ソースコードと当該ソースコードが実行時に使用する、データまたはファイル、例えば、音声、画像、動画データなどを送信する、ソースコード送信処理部201と、を有する。なお、これらの実行時に使用されるデータまたはファイルは、上述の配布データにモバイルコードに添付されるデータやファイルとは異なり、当該モバイルコードがその実行時に必要とするものである。

1 2

次に、検証サーバ120の機能ブロック構成について説明する。

検証サーバ120は、第2図に示すように、作成端末110から前記ソースコードを受信したという情報などを表示装置122に表示させる表示部213と、前記作成端末110から前記ソースコードを受信するソースコード受信処理部211と、を有する。

次に、作成端末110の動作について説明する。

第10図は、作成端末110が、モバイルコード146cの機能検証を、検証サーバ120に依頼する場合の、作成端末110の動作フローを示した図である。

10 まず、前記作成者が入力装置113に前記ソースコードの格納場所と名前、および前記検証サーバ120の位置と名前を入力する(ステップ1001)。次に、ソースコード送信処理部201は、ステップ1002において、指定された前記ソースコードを前記ソースコードファイル202から取り出し、当該ソースコードとソースコードが実行時に使用するデータやファイル
15 を含む機能検証依頼203を作成し、当該機能検証依頼203を、前記作成者が指示した前記検証サーバ120に送信する。

次に、検証サーバ120の動作について説明する。

第11図は、作成端末110が、前記ソースコードの機能検証を、検証サーバ120に依頼する場合の、検証サーバ120の動作フローを示した図である。

20 まず、ステップ1101において、前記ソースコード受信処理部211が、前記作成端末110から前記機能検証依頼203を待ち受ける。前記機能検証依頼203を受信すると、前記ソースコード受信処理部211は、当該機能検証依頼203から取り出した、前記ソースコードをソースコードファイル
25 212に格納し(ステップ1103)、前記作成端末110から前記ソースコードを受信したという情報を、前記表示装置122に表示する(ステップ1104)。

1 3

その後、ステップ1101に遷移し、再び、前記作成端末110から前記機能
検証依頼203を待ち受ける。

次に、検証サーバ120が、前記ソースコードの機能検証、モバイルコ
ード146cの作成と、当該モバイルコード146cの配布サーバ130への登録
5 を行う場合の、検証サーバ120および配布サーバ130の機能ブロック構成
および動作について説明する。

第3図は、検証サーバ120でソースコードの機能を検証し、当該ソース
コードから作成したモバイルコード146cを配布サーバ130に登録する場
合の、検証サーバ120および配布サーバ130の機能ブロック構成を示した
10 図である。ここで、検証サーバ120の各機能ブロックは、検証サーバ120
のCPU125がメモリ126に格納された各プログラムをOSを介して実行する
ことで実現される。また、配布サーバ130の各機能ブロックは、配布サ
ーバ130のCPU135がメモリ136に格納された各プログラムをOSを介して実
行することで実現される。

15 まず、検証サーバ120の機能ブロック構成について説明する。

検証サーバ120は、第3図に示すように、前記検証サーバ120の使用者
(以下、単に検証者とも称する)の指示を受け付ける入力部123と、前記
入力部123に入力されたデータなどを表示する表示装置122と、前記入力
部123から入力された、前記検証者の指示にしたがって、前記記憶装置
20 124に格納された前記ソースコードの機能を検証する、機能検証処理部
301と、前記ソースコードからモバイルコード146cを作成するモバイル
コード作成処理部302と、前記モバイルコード146cの登録を要求するた
め、登録要求305を配布サーバ130に送信する、登録要求送信処理部303
と、を有している。なお、前記登録要求305には、前記モバイルコード
25 作成処理部302が作成した、モバイルコード146cとモバイルコードを格
納する場所を指定する情報が含まれている。

1 4

次に、配布サーバ130の機能ブロック構成について説明する。

配布サーバ130は、第3図に示すように、前記配布サーバ130の使用者
(以下、単に配布者とも称する)の指示を受け付ける入力部133と、前記
入力部133に入力されたデータなどを表示する表示部132と、前記検証サ
5 ーバ120から前記登録要求305を受信し、当該登録要求305に含まれるモ
バイルコード146cを、前記記憶装置134に格納する、登録要求受信処理
部311と、を有している。

次に、検証サーバ120の動作について説明する。

第12図は、検証サーバ120でソースコードの機能を検証し、当該ソー
10 スコードから作成したモバイルコード146cを配布サーバ130に登録する
場合の、検証サーバ120の動作フローを示した図である。

まず、前記検証者が、機能を検証する前記ソースコードの格納場所と
名前を入力部123に入力する(ステップ1201)と、機能検証処理部301は、
前記ソースコードファイル212から指定された前記ソースコードを検索
15 し、当該ソースコードからモバイルコード146cの持つ機能を記述した機
能仕様500を作成する(ステップ1202)。次に、機能仕様確認画面600を前
記表示装置122に表示し(ステップ1203)、ステップ1204に遷移し、前記
検証者の指示を待ち受ける。

第5図は、前記機能検証処理部301が作成する前記機能仕様500の一例
20 を示した図である。この例では、前記ソースコードが、「／etc／
passwd」というファイルに読み込み(501)や書き込み(504)を行ったり、
「／bin／rm」というプログラムを実行したりする(503)などの情報が記
述されている。

また、第6図は、前記機能検証処理部301が前記表示装置122に表示す
25 る、前記機能仕様確認画面600の画面の一例である。前記検証者は、ソ
ースコード表示領域601に表示された前記ソースコードと、機能仕様表

1 5

示領域602に表示された前記機能仕様500とを比較、確認し、前記モバイルコード146cを作成するか否かを選択する。例えば、前記検証者は、前記表示装置122に表示された前記機能仕様500を確認し、当該モバイルコード146cが有害な動作を行うものであると判断した場合には、前記検証者は、キャンセル(拒否)ボタン604を押すなどによって、前記モバイルコード146cの作成を拒否することができる。有害な動作とは例えば、本来の動作には関係のないプログラムを起動している、ユーザー端末からデータを読み込んでサーバに転送しているなどの動作である。なお、作成とは、ソースコードから実行コードを作成(コンパイル)し、機能仕様と実行コードと実行時に使用されるデータやファイルを一つにまとめて(アーカイブして)、さらに署名を付加するという処理を行うことを指す。

ここで、前記検証者が前記モバイルコード146cの作成を拒否するという指示を行った場合には、ステップ1209において、前記ソースコードと、前記機能仕様500とを破棄し、処理を終了する。なお、前記検証者が前記モバイルコード146cの作成を拒否した場合に、前記作成者に対して作成が拒否された旨をその理由と共に通知してもよい。これによって、前記作成者は当該モバイルコード146cの修正すべき箇所を知ることができるという効果がある。

一方、前記検証者が、作成ボタン603を押すなどによって、前記モバイルコード146cの作成を選択した場合には、ステップ1205に遷移する。

また、ステップ1204で、前記検証者が前記機能仕様500を編集することも可能である。前記検証者が編集ボタン605を押すことによって、機能仕様500の編集を選択した場合には、ステップ1210に遷移し、前記機能検証処理部301は、機能仕様編集画面700を前記表示装置122に表示し、前記検証者からの指示を待ち受ける(ステップ1211)。

第7図は、前記機能検証処理部301が前記表示装置122に表示する、前

16

記機能仕様編集画面700の画面の一例である。前記検証者は、この画面を使って、前記機能仕様500の編集を行う。

ここで、更新ボタン702を押すなどによって、編集結果を前記機能仕様500に反映することを選択した場合には、前記機能検証処理部301は、
5 編集結果を反映した機能仕様500を新たに作成し(ステップ1212)、ステップ1204に戻る。

一方、キャンセルボタン703を押すなどによって、編集結果を前記機能仕様500に反映しないことを選択した場合には、そのまま、ステップ1204に戻る。

10 ステップ1205では、前記機能仕様500と、検証サーバが作成した前記モバイルコード146cを特定するためのモバイルコード識別子と、の組を機能仕様登録ファイル304に格納し、前記モバイルコード作成処理部302に処理を移す。

前記モバイルコード作成処理部302は、ステップ1206で、実行コード
15 と、検証者の署名とを生成し、モバイルコード146cを作成する。

次に、ステップ1207で、前記検証者が、前記モバイルコード146cを登録する配布サーバ130の名前とその中の格納場所を入力すると、前記登録要求送信処理部303は、前記モバイルコード146cと、その格納場所などを含んだ登録要求305を作成し、指定された配布サーバ130に、前記登録要求305を送信し(ステップ1208)、処理を終了する。なお、前記モバイルコード146cを前記配布サーバ130に登録した場合に、前記作成者に対してその旨を通知してもよい。これにより、前記作成者は前記モバイルコード146cが確かに作成されたことを知ることができるという効果がある。
20

25 次に、配布サーバ130の動作について説明する。

第13図は、検証サーバ120でソースコードの機能を検証し、当該ソー

1 7

スコードから作成した当該モバイルコード146cを配布サーバ130に登録する場合の、配布サーバ130の動作フローを示した図である。

まず、ステップ1301において、前記登録要求受信処理部311が、前記検証サーバ120から前記登録要求305を待ち受ける。前記登録要求305を受信する(ステップ1302)と、前記登録要求受信処理部311は、前記登録要求305に含まれるモバイルコード146cを、指定された格納場所に格納し(ステップ1303)、前記検証サーバ120から前記モバイルコード146cを受信したという情報を、前記表示部132に表示する(ステップ1304)。その後、ステップ1301に遷移し、再び、前記検証サーバ120から前記登録要求305を待ち受ける。

次に、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、ユーザー端末140および配布サーバ130の機能ブロック構成および動作について説明する。

第4図は、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取る際の、ユーザー端末140および配布サーバ130の機能ブロック構成を示す図である。ここで、ユーザー端末140の各機能ブロックは、ユーザー端末140のCPU145がメモリ146に格納された各プログラムをOSを介して実行することで実現される。また、配布サーバ130の各機能ブロックは、配布サーバ130のCPU135がメモリ136に格納された各プログラムをOSを介して実行することで実現される。

まず、ユーザー端末140の機能ブロック構成について説明する。

ユーザー端末140は、第4図に示すように、前記ユーザー端末140の使用者(以下、単にユーザーとも称する)の指示を受け付ける入力部143と、前記入力部143に入力されたデータや、配布サーバ130から送られてきたデータなどを表示する表示部142と、前記入力部143に入力された前記ユ

18

ーザーの指示にしたがい、配布サーバ130に対してモバイルコード146c
の配送要求417を送信する、要求送信処理部411と、前記配布サーバ130
からモバイルコード146cを受信するモバイルコード受信処理部412と、
前記モバイルコード146cに付加された署名を検証する署名検証処理部
5 413と、前記モバイルコード146cの機能を確認する機能確認処理部414と、
前記モバイルコード146cを実行するモバイルコード実行処理部415と、
を有する。

次に、配布サーバ130の機能ブロック構成について説明する。

配布サーバ130は、第4図に示すように、ユーザー端末140から前記配
10 送要求417を受け付ける要求受信処理部401と、当該配送要求417にした
がい、モバイルコード146cを含む上記配布データを前記ユーザー端末
140に送信するモバイルコード送信処理部402と、を有する。

次に、ユーザー端末140の動作について説明する。

第14図は、ユーザー端末140が、配布サーバ130からモバイルコード
15 146cを含む上記配布データを受け取り、当該モバイルコード146cを実行
する際の、ユーザー端末140の動作フローを示した図である。

まず、前記モバイルコード146cの名前や格納場所を示す情報(ファイ
ル名やディレクトリ名など)を用いて、前記配布サーバ130に置かれてい
るモバイルコード146cなどのダウンロードが指示される(ステップ1401)
20 と、要求送信処理部411は、前記配布サーバ130に、前記モバイルコード
146cの配送要求417を送信する(ステップ1402)。前記モバイルコード
146cの名前や格納場所を示す情報としては、例えば、本実施形態のよう
に、Browserプログラムを利用してデータを受信する場合には、配布デ
ータの名前や格納場所を示す情報として、配布サーバ130のアドレスと
25 ファイル名とを連結した、いわゆるUniform Resource
Locators(URLs)を用いる。

次に、ステップ1403において、前記モバイルコード受信処理部412が、前記配布サーバ130からの配付データを待ち受け、前記配布サーバ130から、前記モバイルコード146cなどを受け取ると、前記署名検証処理部413に処理を移す。ステップ1404において、前記署名検証処理部413は、
5 前記モバイルコード146cに付加されている、前記検証者の署名を検証する上記ダウンロードの指示方法として、

(1) 前記ユーザがURLを明示的に指定する

(2) 閲覧中のHTMLファイルにモバイルコードのURLが指定されていて、Browserプログラム146bが自動的にダウンロード指示を出す

10 がある。また、

(3) 配布サーバ130がPUSH技術を用いて、モバイルコード146cを送付してくる場合もある

が、このとき、ステップ1401、1402は省略される。

ここで、前記モバイルコード146cの完全性(前記検証サーバ120が当該
15 モバイルコード146cを作成した時点から当該モバイルコード146cに対して改ざんがなされていない)が確認できなかった場合や、前記検証者を信頼することができないと判断した場合には、その旨を表示部142に表示した後(ステップ1412)、ステップ1413に移行し、処理を終了する。なお、検証者を信頼することができるか否かを判断する方法については、
20 従来の署名付きコードにおいて、その署名者を信頼できるか否かを判断する方法と同じであり、詳細な説明は省略する。

一方、ステップ1405において、前記モバイルコード146cの完全性が確認され、かつ、前記検証者を信頼できると判断した場合には、前記機能確認処理部414に処理を移す。前記機能確認処理部414は、前記
25 モバイルコード146cから、当該モバイルコード146cの機能仕様500を取り出し(ステップ1406)、記憶装置144の機能仕様管理ファイル416に記録

20

された、第9図に示すようなテーブルに同じ機能仕様500が登録されているか否かを確認する(ステップ1407)。

5 なお、機能仕様管理ファイル416は、機能仕様500が、その実行が許可される度に順次登録された、あるいは、信頼できる、第3者やシステムの管理者によって、あらかじめ配布された、実行が許可された実績のある(すなわち安全な)機能仕様を格納したファイルである。第9図は、安全な機能仕様500が、順番に番号が付けられて前記機能仕様管理ファイル416に登録されている例を示している。

10 ここで、前記機能仕様管理ファイル416に同じ機能仕様500が登録されている場合には、ステップ1411に移行し、前記モバイルコード実行処理部415に処理を移す。

15 一方、同じ機能仕様500が前記機能仕様管理ファイル416に登録されていない場合には、ステップ1408で、表示部142に、実行確認画面800を表示し、当該モバイルコード146cを実行するか否かの指示を前記ユーザーに求める。

20 第8図は、前記実行確認画面800の一例である。この例では、現在実行しようとしているモバイルコード146cが「／etc／passwd」というファイルからデータを読み込んだり(811)、読み込んだデータをwww.foo.co.jpというコンピュータに転送する(813)などの情報が表示される。また、第20図は、前記実行確認画面800の他の一例である。この例では、現在実行しようとしているモバイルコード146cが「／etc／passwd」というファイルに読み込み(2011)や書き込み(2014)を行ったり、「／bin／rm」というプログラムを実行(2015)したりするなどの情報が表示されている。

25 いずれの場合も、前記ユーザーは、画面に表示された情報により、現在実行しようとしている前記モバイルコード146cの機能を確認し、当該

2 1

モバイルコード146cの実行を許可するか否かを選択する。

ここで、前記ユーザーが、実行ボタン820を押すなど、入力部142から、前記モバイルコード146cを実行するという指示を入力した場合には、前記機能確認処理部414は、前記機能仕様管理ファイル416に、前記モバイルコード146cの機能仕様500を新規に追加し(ステップ1410)、ステップ1411に移行して、前記モバイルコード実行処理部415に処理を移行する。

一方、前記ユーザーが拒否ボタン830を押すなど、入力部142から、前記モバイルコード146cの実行を認めないという指示を入力した場合には、ステップ1413に移行する。

10 ステップ1411では、モバイルコード実行処理部414が前記モバイルコード146cを実行する。なお、本実施例におけるモバイルコード146cの実行とは、当該モバイルコードに含まれる実行コードの実行を意味する。

次に、配布サーバ130の動作について説明する。

15 第15図は、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、配布サーバ130の動作フローを示した図である。

20 まず、ステップ1501で、前記要求受信処理部401が、前記ユーザー端末140から配送要求417を待ち受け、前記ユーザー端末140から配送要求417を受信すると、前記モバイルコード送信処理部402に処理を移す。前記モバイルコード送信処理部402は、当該配送要求417に応じた前記モバイルコード146cを、必要に応じてマルチメディアファイルなどを添付して、前記ユーザー端末140に送信する(ステップ1503)。その後、ステップ1501に戻って、再び、前記ユーザー端末140から配送要求417を待ち受ける。

25 以上述べたように、本実施例では、モバイルコード146cには、検証サーバ120によって作成された、当該モバイルコード146cの持つ機能を記

2 2

述した機能仕様500が含まれている。ユーザー端末140が、配布サーバ130からモバイルコード146cを受信した場合、前記モバイルコード146cを実行する前に、当該モバイルコード146cから取り出した前記機能仕様500を、それが実行許可されたものでない場合でも、前記ユーザーに提示し、当該モバイルコード146cを実行するか否かを選択させる。このため、前記ユーザー端末140は、モバイルコード146cの持つ機能に基づいて、当該モバイルコード146cを実行するか否かを決定することができる。

次に、本発明の他の実施形態として、機能仕様500を検証サーバ120で集中管理する実施形態について説明する。

10 本実施形態では、モバイルコード146cには、当該モバイルコード146cの実行コード以外に、当該モバイルコード146cを他と区別するためのモバイルコード識別子や、前記検証者の署名(本実施形態でも署名を検証するために必要なすべてのデータをまとめて署名と記述する)や、モバイルコード自身が使用するデータやファイルが含まれており、モバイルコード146c自体の完全性の確認に利用可能である。

なお、機能仕様500を検証サーバ120で集中管理する実施形態のシステムの機器概略構成、およびハードウェア構成は、前述の、モバイルコード146cに機能仕様500が含まれる実施形態と同じであり、その詳細な説明は省略する。

20 同様に、前記作成者が作成端末110で前記ソースコードを作成する場合の、前記作成端末110の機能ブロック構成、および動作については、従来のモバイルコードシステムと同じであり、その詳細な説明は省略する。

同様に、作成端末110が、モバイルコード146cの機能検証を、検証サーバ120に依頼する場合の、前記作成端末110、および前記検証サーバ120の機能ブロック構成、および動作については、前述の、モバイルコ

23

ード146cに機能仕様500が含まれる実施形態と同じであり、その詳細な説明は省略する。

また、検証サーバ120でモバイルコード146cの機能検証を行い、配布サーバ130に登録する場合の、前記検証サーバ120、および前記配布サーバ130の機能ブロック構成、および動作については、第12図のステップ1206においてモバイルコード146cを作成する際に、機能仕様500の代わりに当該機能仕様500と対応づけて作成したモバイルコード識別子を用いる以外は、前述の、モバイルコード146cに機能仕様500が含まれる実施形態と同じであり、その詳細な説明は省略する。

10 まず、本実施例において、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、検証サーバ120、ユーザー端末140、および配布サーバ130の機能ブロック構成および動作について説明する。

15 第16図は、本実施例において、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、検証サーバ120、配布サーバ130、およびユーザー端末140の機能ブロック構成を示した図である。

20 検証サーバ120は、第16図に示すように、ユーザー端末140から機能仕様要求418を受信し、当該ユーザー端末140に要求された機能仕様500を送信する、機能仕様送信処理部1621を有している。

25 なお、第16図において、ユーザー端末140、および配布サーバ130の機能ブロック構成は、第4図に示したものと同じであり、その詳細な説明は省略する。ただし、本実施例では、ユーザー端末140の機能確認処理部414は、前記検証サーバ120に機能仕様要求418を送信し、前記検証サーバ120から機能仕様500を受信するという処理も行う。

次に、ユーザー端末140の動作について説明する。

24

第17図は、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、ユーザー端末140の動作フローを示した図である。

この図において、ステップ1401からステップ1405とステップ1407から
5 ステップ1412までは第14図と同じであり、説明を省略する。

ステップ1405の判断結果により、前記機能確認処理部414に処理が移ると、

前記機能確認処理部414は、前記モバイルコード146cから、モバイルコード識別子を取り出し、当該モバイルコード識別子を含む、機能仕様要求418を前記配布サーバ120に送信する(ステップ1701)。ステップ1702で、
10 前記配布サーバ120から前記モバイルコード識別子に対応する機能仕様500を受信すると、あらかじめ記憶装置144の機能仕様管理ファイル416に記憶された、第9図に示したようなテーブルに同じ機能仕様500が登録されているか否かを確認する(ステップ1407)。

15 以下のステップの動作は、第14図と同じなので、説明を省略する。

次に、検証サーバ120の動作について説明する。

第18図は、ユーザー端末140が、配布サーバ130からモバイルコード146cを含む上記配布データを受け取り、当該モバイルコード146cを実行する際の、前記検証サーバ120の動作フローを示した図である。

20 まず、仕様送信処理部1621は、ステップ1801で、前記ユーザー端末140から前記機能仕様要求418を待ち受ける。前記機能仕様要求418を受信した場合には、前記機能仕様要求418に含まれているモバイルコード識別子を取り出し(ステップ1803)、機能仕様登録ファイル304から、当該モバイルコード識別子に対応する機能仕様500を検索する(ステップ
25 1804)。前記機能仕様500を、前記ユーザー端末140に送信し(ステップ1805)、ステップ1801に戻り、再度、前記ユーザー端末140から前記機能

25

仕様要求418を待ち受ける。

なお、配布サーバ130の動作については、前述の、モバイルコード146cに機能仕様500が含まれる実施形態と同じであり、その詳細な説明は省略する。

- 5 以上述べたように、本実施例では、検証サーバ120が、ソースコードの機能を検証した際に作成した、機能仕様500と前記モバイルコード146cを一意に特定するためのモバイルコード識別子との組を管理している。かつ、モバイルコード146cには、前記モバイルコード識別子が含まれており、ユーザー端末140が、配布サーバ130からモバイルコード146c
10 を受信した場合、まず、モバイルコード146cから取り出したモバイルコード識別子を検証サーバ120に送信する。モバイルコード識別子を受信した検証サーバ120では、モバイルコード識別子に対応する機能仕様500を検索し、前記ユーザー端末140に返信する。前記機能仕様500を受信した前記ユーザー端末140は、当該機能仕様500が許可済みの機能仕様でな
15 ければ、それを前記ユーザーに提示し、当該モバイルコード146cを実行するか否かを選択させる。このため、前記ユーザー端末140は、モバイルコード146cの持つ機能に基づいて、当該モバイルコード146cを実行するか否かを決定することができる。

- 20 なお、以上の各実施例において、各プログラムが行う、種々の「要求」、「依頼」を含む通信は、周知のプログラム(あるいは、モジュール、プロセス)間の通信技術(たとえば、“ソケット”が知られている)を使用することで実現できるものである。

また、各プログラムが行う送受信は、各計算機ハードウェアのOSと、通信網インタフェースと、通信網を介して行われるものである。

- 25 また、各表示装置への表示や入力装置からの入力は、それぞれ、表示部や入力部のプログラムが、OSを介して、あるいは、直接に行うもので

26

ある。

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

たとえば、上記の実施形態では、検証サーバ120と、配布サーバ130と、
5 は異なる計算機ハードウェア上に構成しているが、本発明はこれに限定
されない。すなわち、検証サーバ120と、配布サーバ130と、を同じ計算
機ハードウェア上に構成してもよい。同様に、作成端末110と、検証サ
ーバ120と、を同じ計算機ハードウェア上に構成してもよい。同様に、
作成端末110と、配布サーバ130と、を同じ計算機ハードウェア上に構成
10 してもよい。さらには、作成端末110と、検証サーバ120と、配布サーバ
130と、を同じ計算機ハードウェア上に構成してもよい。これらの場合、
各サーバ、端末の機能を実現するプログラムは、同じ計算機ハードウェ
ア上で、OSにより互いに独立したプログラム(プロセス)として、その動
作が管理されることになる。

15 また、検証サーバ120は、作成した前記モバイルコード146cを作成端
末110に送信し、作成端末110が配布サーバ130に登録するようにしても
よい。このようにすることで、作成者はモバイルコード146cに登録する
配布サーバ130を選択することができる。

また、作成端末110は、前記ソースコードを配布サーバ130に登録し、
20 配布サーバ130が、検証サーバ120にモバイルコード146cの機能検証を依
頼するようにしてもよい。このようにすることで、配布者は自らが信頼
する検証者に機能検証を依頼することができる。

また、前記作成端末110において、作成者が前記機能仕様500を作成し、
前記ソースコードと共に当該機能仕様500を、検証サーバ120に送信する
25 ようにしてもよい。このようにすることで、検証者は、前記機能仕様
500が不正な動作をするものでないことと、前記ソースコードが当該機

27

能仕様500の通りに実装されたものであることと、を確認することによって、モバイルコード146cが不正な動作を行うものでないことを保証することができる。検証者サーバ120に機能仕様500を作成する機能は不要となる。

- 5 また、検証者に機能を確認させる前に、不正な処理を行うモバイルコード146cの機能仕様500の特徴を、リストにまとめ、検証サーバ120の記憶装置124に保存しておいてもよい。そして検証対象となっているソースコードから作成する機能仕様500が、前記リストに該当する特徴を持つか否かを確認することによって、当該モバイルコード146cが不正な処理を行うか否かを確認する処理を組み込んでもよい。このようにすることで、既知の不正処理手法を用いた、前記リストに該当するモバイルコード146cについては、検証者が機能検証を行う手間を省くことができるので、効率がよくなる。

- 15 また、前記作成端末110は、検証サーバ120に対し、前記モバイルコード146cの実行コードと機能仕様を送信するようにしてもよい。この場合、第12図においてステップ1202が不要となる。またステップ1201の「ソースコード指定」が「実行コード指定」に、ステップ1209の「ソースコード破棄」が「実行コード破棄」に変更される。さらに、ステップ1206において、ソースコードから実行コードをコンパイルする機能を不要とすることができる。

- 20 また、上記の実施形態では、作成端末110と、検証サーバ120と、配布サーバ130と、ユーザー端末140と、の間で、通信網100を介してやり取りされる情報の機密性や完全性の確保について特別な手段を用いていないが、本発明は、様々な暗号手段や認証手段を併用することを妨げるものではない。通信網100を流れる情報に対して、暗号手段や認証手段を適用することにより、システム全体の安全性をさらに高めることができ

る。

また、上記の実施形態では、前記ユーザーが実行を許可したモバイルコード146cは、他のプログラムを自由に起動するなど、ユーザー端末110のあらゆるリソースを使用することができると仮定している。しかし、たとえば、モバイルコード146cが他のプログラムに各種サービスを要求する場合には、Browserプログラム146b、またはOS146aが、機能仕様500を前記他のプログラムに渡すようにし、前記機能仕様500を渡されたプログラムは、モバイルコード146cからの要求を実行するか否かを、当該機能仕様500に基づいて判断するようにしてもよい。

- 10 また、上記の実施形態では、作成端末110と検証サーバ120との間のデータのやり取りは、通信網100を介して行うようにしているが、本発明はこれに限定されない。作成端末110で作成した前記ソースコードをフロッピーディスクなどの記憶媒体に記録し、前記検証者に渡すようにしてもよい。同様に、検証サーバ120と配布サーバ130との間のデータのやり取りも、モバイルコード146cを記憶媒体に記録し、前記配布者に渡すようにしてもよい。
- 15

産業上の利用可能性

- 以上説明したように、本発明によれば、モバイルコードが持っている機能に基づいて、当該モバイルコードを実行するか否かを決定することができるのでより安全である。
- 20

請求の範囲

1.

モバイルコードの実行方法であって、

モバイルコードを取得する、モバイルコード取得ステップと、

- 5 前記取得した前記モバイルコードに付加されている署名を検証する、
署名検証ステップと、

前記署名検証ステップによって、当該モバイルコードの署名の検証に
成功した場合に、当該モバイルコードの持つ機能を記述した機能仕様を
取得する機能仕様取得ステップと、

- 10 前記取得した前記機能仕様によって、前記モバイルコードの持つ機能
を確認し、当該モバイルコードの実行を許可するか否かを判断する、機
能確認ステップと、

前記機能確認ステップによって、前記モバイルコードの実行が許可され
た場合に、前記モバイルコードを実行するモバイルコード実行ステップ

- 15 と

を備えたモバイルコードの実行方法。

2.

請求項1記載のモバイルコードの実行方法であって、

- 20 前記機能確認ステップは、前記機能仕様をユーザーに提示し、前記ユ
ーザーが当該機能仕様を持つモバイルコードの実行を許可すると判断し
た場合に、前記モバイルコードの実行を許可すると判断するものである
こと

を特徴とするモバイルコードの実行方法。

25

3.

30

請求項 1 または 2 記載のモバイルコードの実行方法であって、

前記機能確認ステップは、前記機能仕様が、実行を許可する機能仕様を格納した、機能仕様管理ファイルに登録されている場合に、前記モバイルコードの実行を許可すると判断するステップを含むこと

5 を特徴とするモバイルコードの実行方法。

4 .

請求項 3 記載のモバイルコードの実行方法であって、

10 前記機能確認ステップは、前記モバイルコードの実行を許可すると判断した場合に、前記機能仕様管理ファイルに前記機能仕様を追加するものであること

を特徴とするモバイルコードの実行方法。

5 .

15 請求項 1 ないし 4 いずれかーに記載のモバイルコードの実行方法であって、

前記モバイルコードは、当該モバイルコードの実行コードと、前記署名と、前記機能仕様と、を含み、

20 前記機能仕様取得ステップは、前記モバイルコードから前記機能仕様を取り出すステップをさらに含むこと

を特徴とするモバイルコードの実行方法。

6 .

25 請求項 1 ないし 4 いずれかーに記載のモバイルコードの実行方法であって、

前記モバイルコードは、当該モバイルコードの実行コードと、前記署

3 1

名と、当該モバイルコードを識別する、モバイルコード識別子と、を含み、

前記機能仕様取得ステップは、前記モバイルコード識別子に対応する機能仕様を、機能仕様登録ファイルから取得すること

5 を特徴とするモバイルコードの実行方法。

7 .

請求項 6 記載のモバイルコードの実行方法であって、

10 前記機能仕様登録ファイルは、信頼できる第三者機関が、前記モバイルコード識別子と当該モバイルコード識別子に対応する前記機能仕様とを組として保管するものであって、

前記機能仕様取得ステップは、前記信頼できる第三者機関から、前記モバイルコード識別子に対応する機能仕様を取得すること

を特徴とするモバイルコードの実行方法。

15

8 .

請求項 5 ないし 7 いずれか一に記載のモバイルコードの実行方法であって、

前記機能仕様は、信頼できる第三者機関が作成したものであり、

20 前記署名は前記信頼できる第三者機関の署名であること
を特徴とするモバイルコードの実行方法。

9 .

25 モバイルコードのソースコードを作成する、ソースコード作成端末と、
ソースコードの機能を検証する、機能検証サーバと、モバイルコードを配布する、モバイルコード配布サーバと、モバイルコードを実行する、

3 2

ユーザー端末と、からなるモバイルコードシステムであって、

前記ソースコード作成端末は、

モバイルコードのソースコードを作成するソースコード作成手段と、

前記モバイルコードのソースコードを前記機能検証サーバに送信する

5 ソースコード送信手段と、

を備え、

前記機能検証サーバは、

送信された前記モバイルコードのソースコードから当該モバイルコードの持つ機能を記述した機能仕様を作成し、当該モバイルコードが不正

10 な処理を行うものでないかを検証する機能検証手段と、

前記機能検証手段が前記モバイルコードは不正な処理を行うものではないと判断した場合に、前記ソースコードから前記モバイルコードを作成するモバイルコード作成手段と、

前記配布サーバに対して、前記モバイルコード作成手段によって作成
15 された、モバイルコードの登録を要求する登録要求手段と、

を備え、

前記モバイルコード配布サーバは、

前記登録を要求された前記モバイルコードを格納し、保管するモバイルコード保管手段と、

20 前記ユーザー端末から配送を要求された、前記モバイルコード保管手段が保管している前記モバイルコードを前記ユーザー端末に送信するモバイルコード送信手段と、

を備え、

前記ユーザー端末は、

25 前記モバイルコード配布サーバに対して、モバイルコードの配送を要求する配送要求送信手段と、

3 3

配送されたモバイルコードに付加されている電子的な署名を検証する署名検証手段と、

前記署名検証手段が署名の検証に成功した場合、前記検証サーバの機能検査手段が作成した前記機能仕様を取得し、当該機能仕様によって前記モバイルコードの持つ機能を確認し、当該モバイルコードの実行を許可するか否かを判断する機能確認手段と、

前記機能確認手段が前記モバイルコードの実行を許可すると判断した場合に、前記モバイルコードを実行するモバイルコード実行手段と、
を備えていることを特徴とするモバイルコードシステム。

10

1 0 .

請求項 9 記載のモバイルコードシステムであって、

前記機能確認手段は、前記機能仕様をユーザーに提示し、前記ユーザーが当該機能仕様を持つモバイルコードの実行を許可すると判断した場合に、前記モバイルコードの実行を許可すると判断すること
を特徴とするモバイルコードシステム。

15

1 1 .

請求項 9 または 1 0 記載のモバイルコードシステムであって、

前記機能確認手段は、前記機能仕様が、実行を許可する機能仕様を格納した、機能仕様管理ファイルに予め登録されている場合に、前記モバイルコードの実行を許可すると判断する手段を備えること
を特徴とするモバイルコードシステム。

20

1 2 .

請求項 1 1 記載のモバイルコードシステムであって、

25

3 4

前記機能確認手段は、前記モバイルコードの実行を許可すると判断した場合に、前記機能仕様管理ファイルに前記機能仕様を追加する手段を備えること

を特徴とするモバイルコードシステム。

5

1 3 .

請求項 9 ないし 1 2 いずれかに記載のモバイルコードシステムであって、

前記モバイルコードは、当該モバイルコードの実行コードと、前記署名と、前記機能仕様と、を含み、

10

前記機能確認手段は、前記モバイルコードから前記機能仕様を取得する手段を備えること

を特徴とするモバイルコードシステム。

15 1 4 .

請求項 9 ないし 1 2 いずれかに記載のモバイルコードシステムであって、

前記モバイルコードは、当該モバイルコードの実行コードと、前記署名と、当該モバイルコードを識別する、モバイルコード識別子と、を含み、

20

前記機能確認手段は、前記モバイルコード識別子に対応する機能仕様を、機能仕様登録ファイルから取得する手段を備えること

を特徴とするモバイルコードシステム。

25 1 5 .

請求項 1 4 記載のモバイルコードシステムであって、

3 5

前記機能仕様を取得する手段は、前記機能検証サーバに前記モバイルコード識別子を送信する手段を備え、

前記機能検証サーバは、

- 5 前記機能仕様登録ファイルとして、モバイルコード識別子と当該モバイルコード識別子に対応する前記機能仕様との組を保管する機能仕様保管手段と、

前記ユーザー端末から受信したモバイルコード識別子に対応する機能仕様を前記機能仕様登録ファイルから検索する手段と、

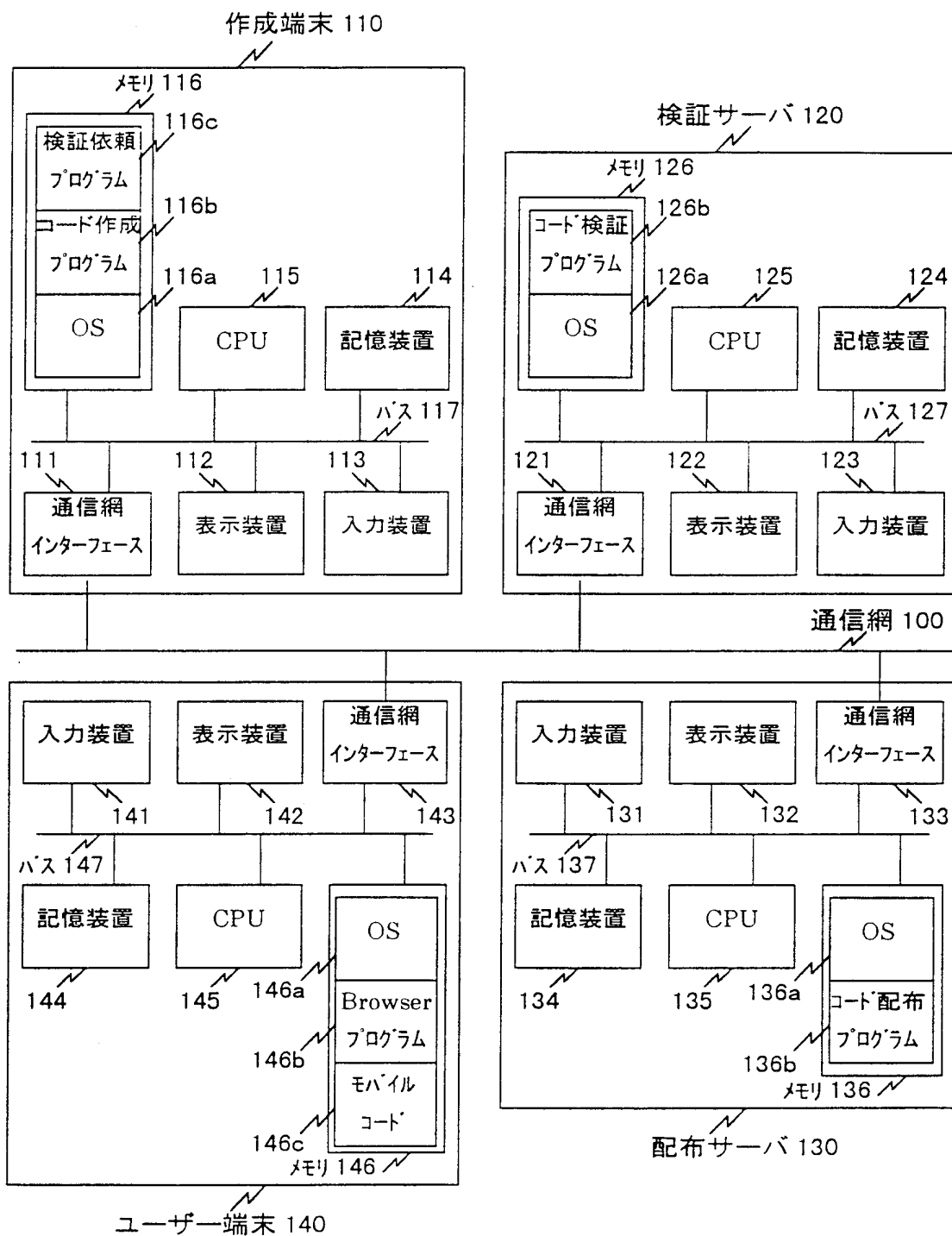
- 10 検索した機能仕様を前記ユーザー端末に送信する機能仕様送信手段と、
を備えること
を特徴とするモバイルコードシステム。

1 6 .

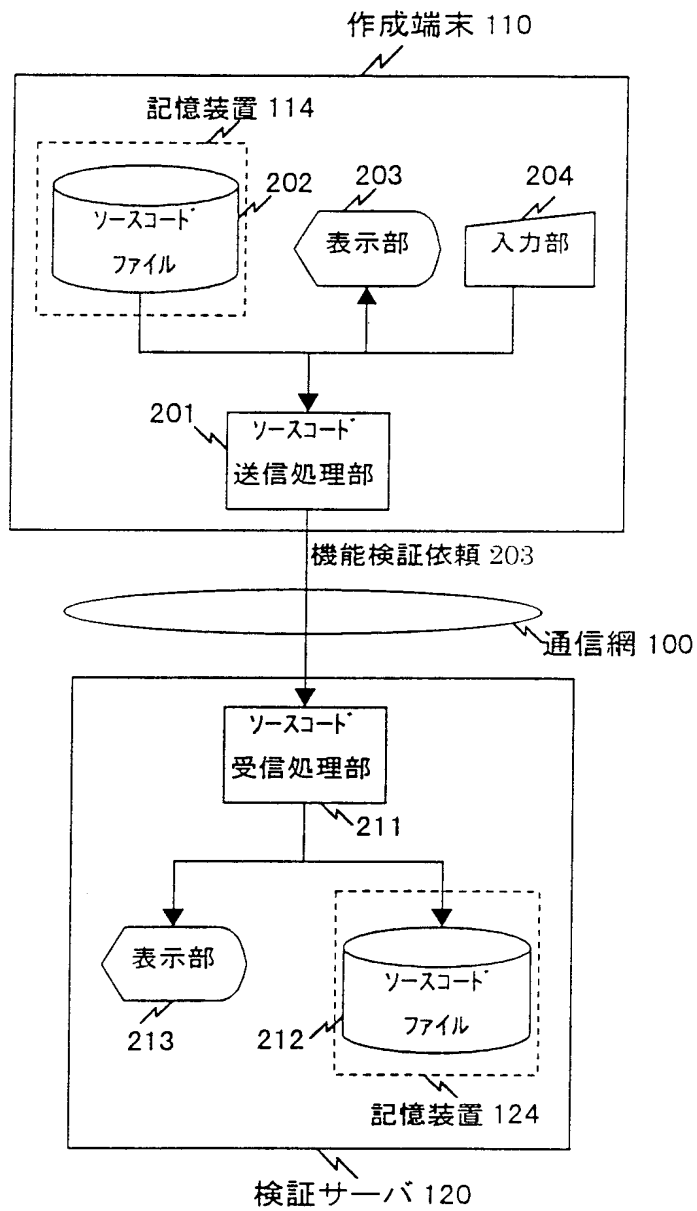
- 15 請求項 1 3 ないし 1 5 いずれかーに記載のモバイルコードシステムであって、

前記署名は前記機能検証サーバが生成し、付加すること
を特徴とするモバイルコードシステム。

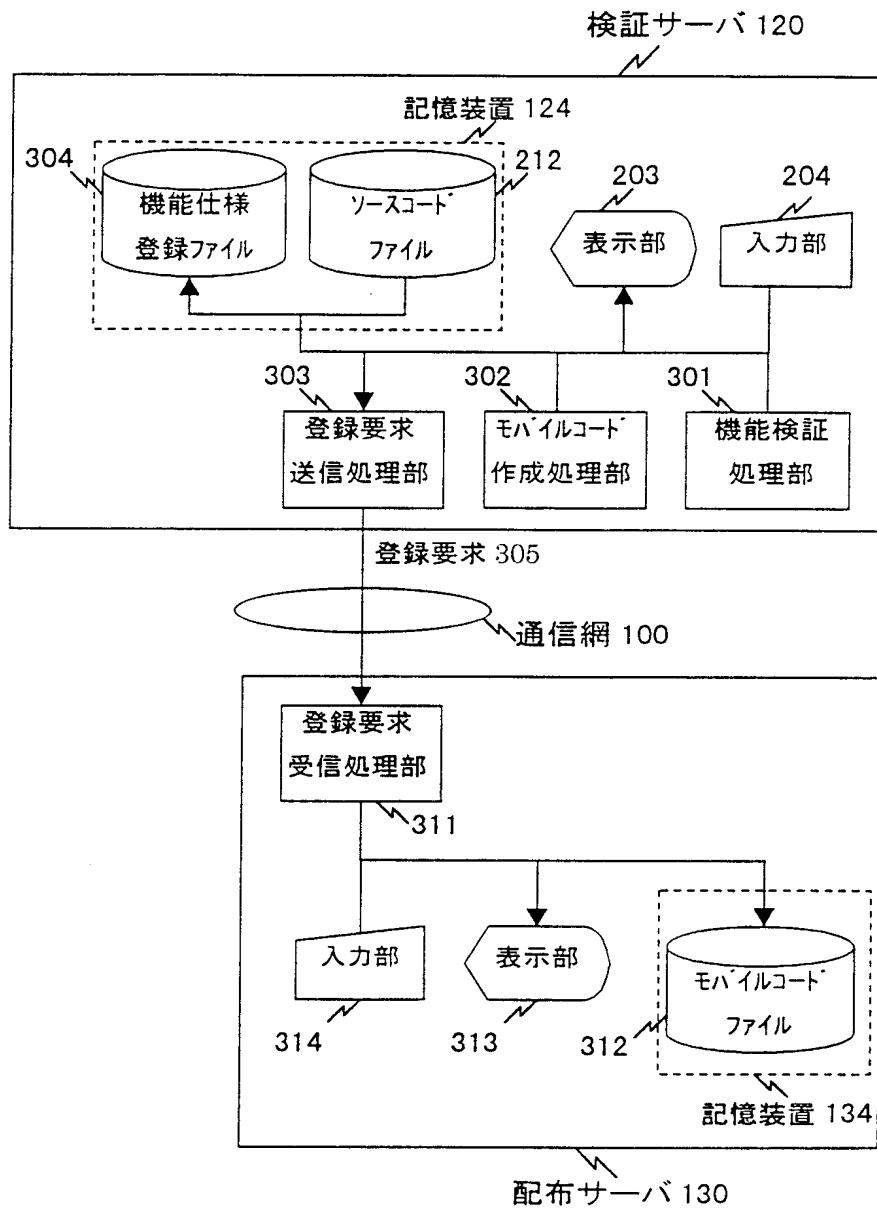
第 1 図



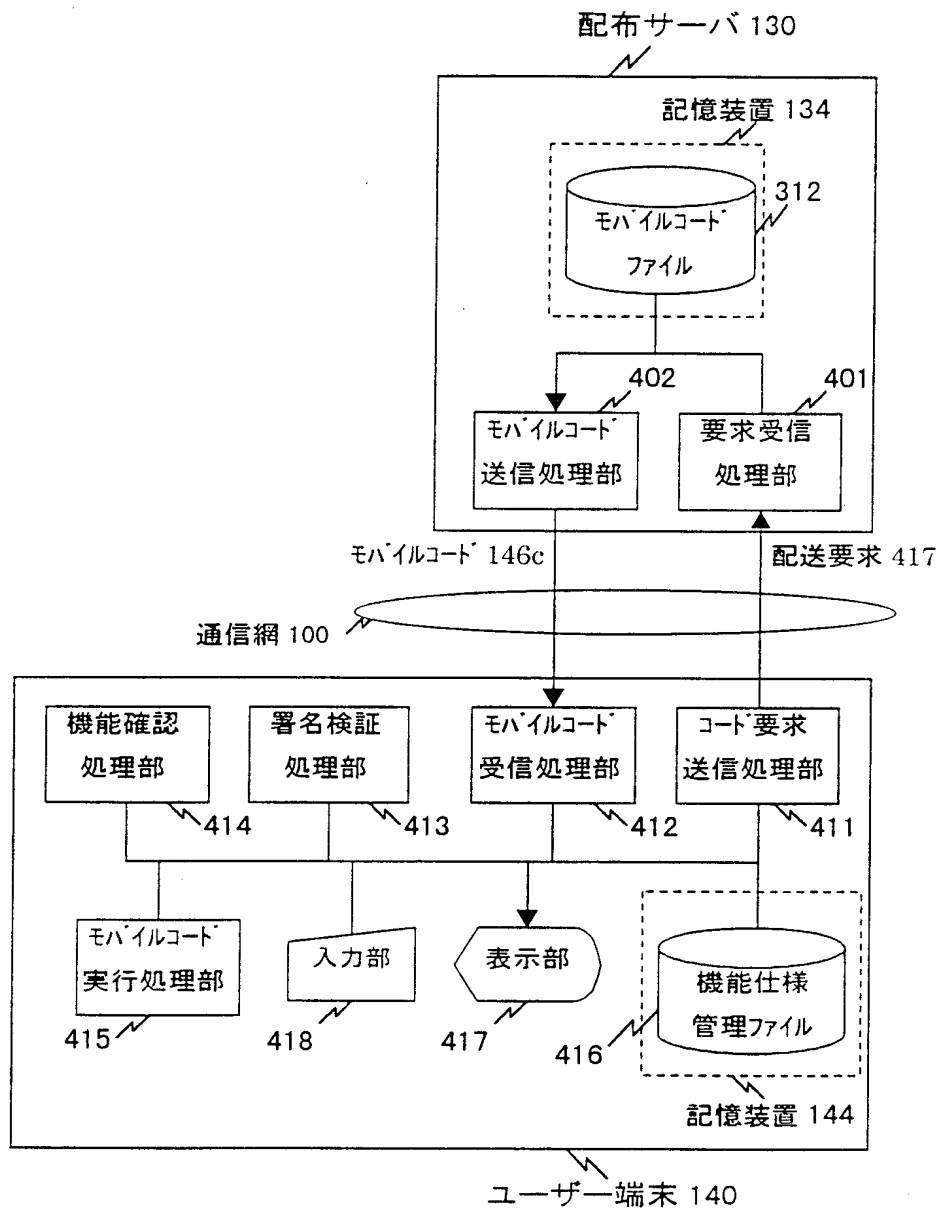
第 2 図



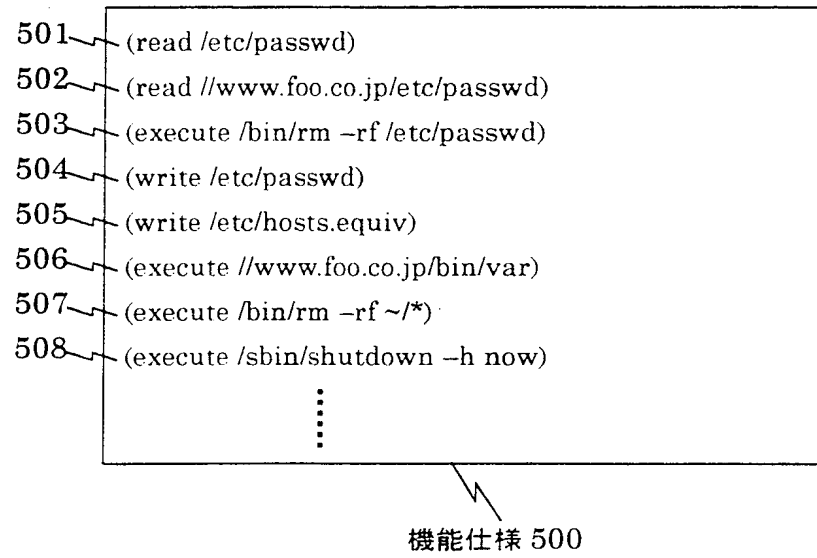
第 3 図



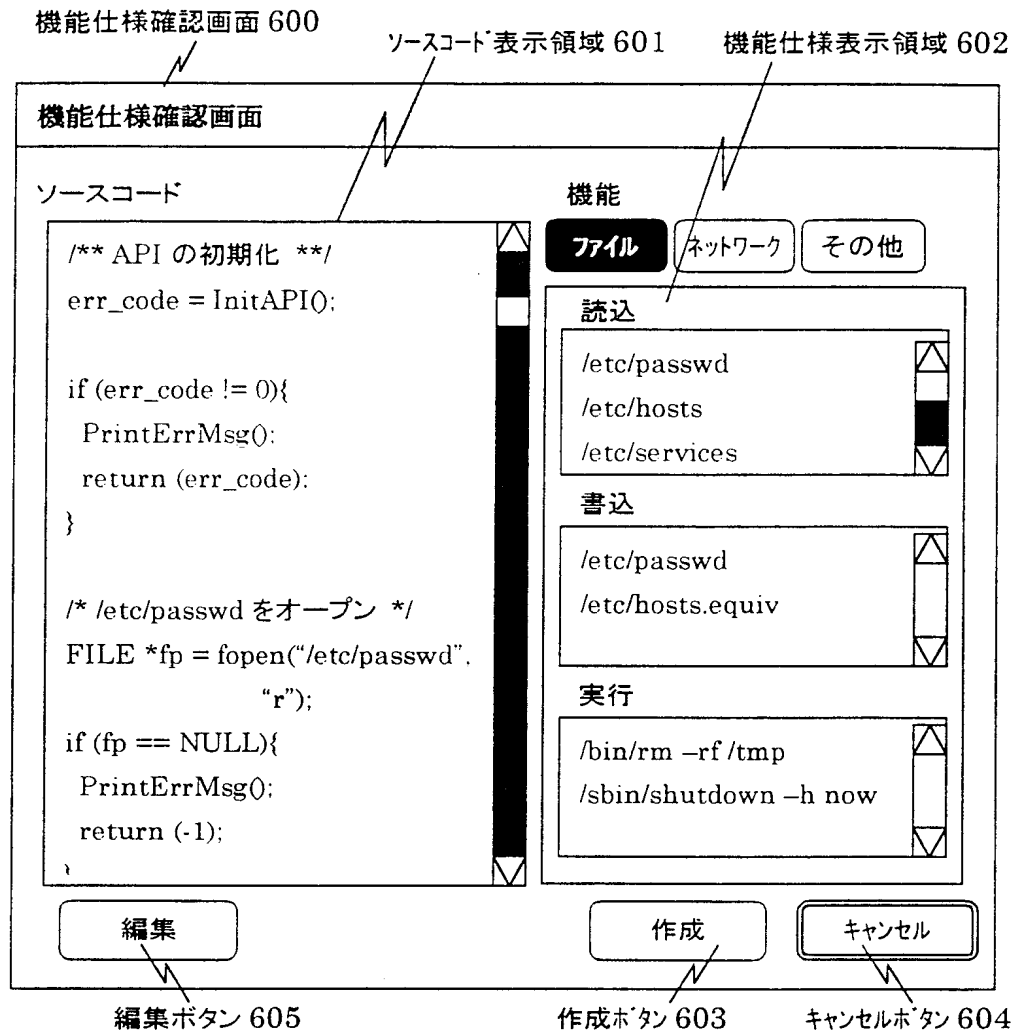
第 4 図



第 5 図

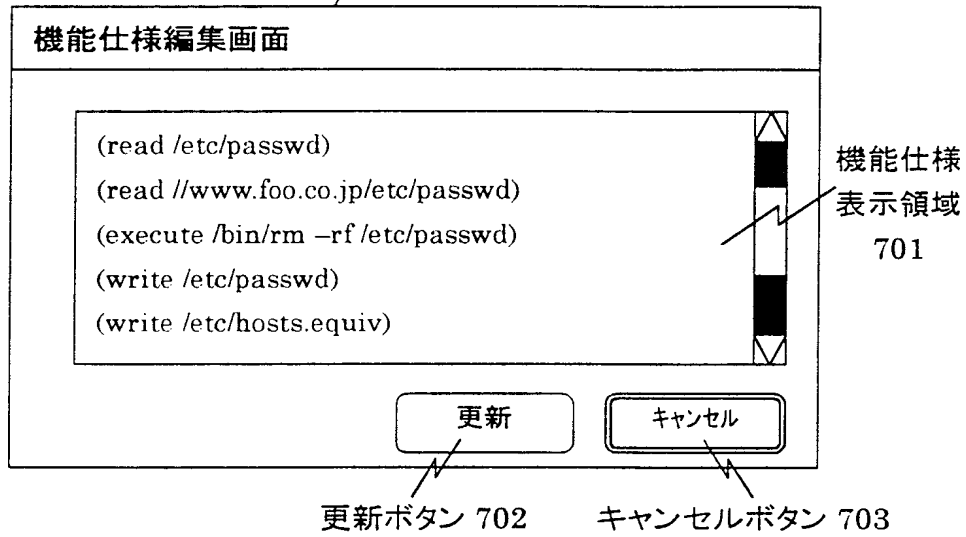


第 6 図



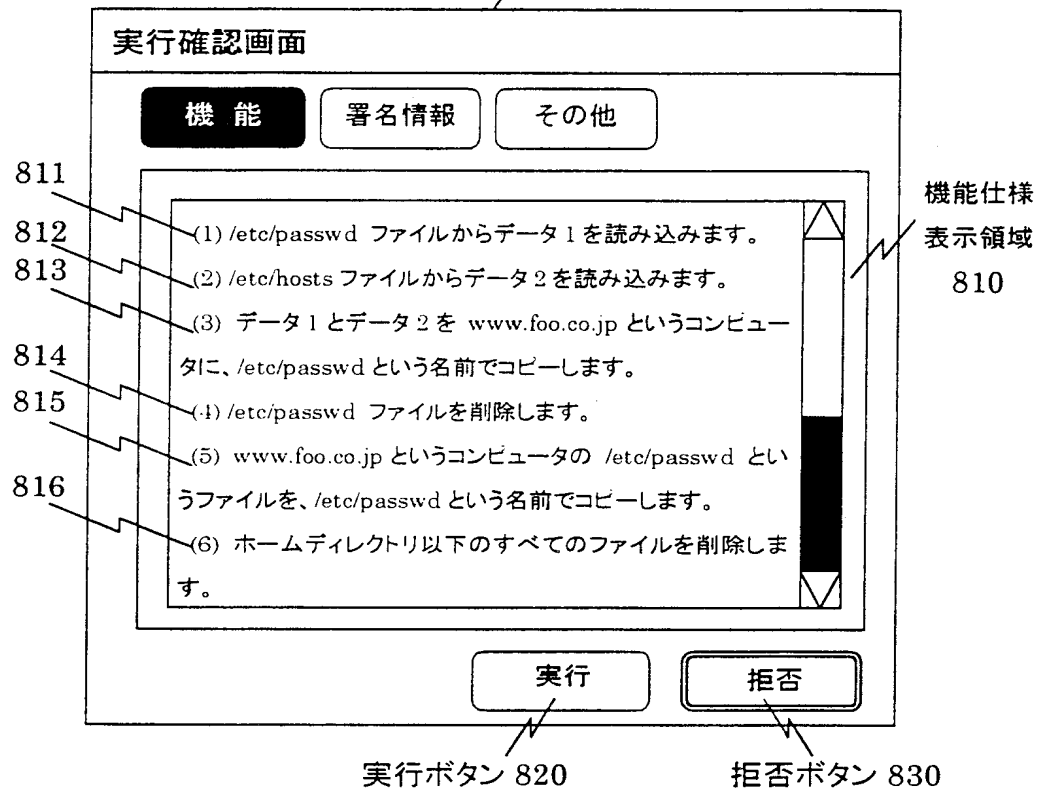
第 7 図

機能仕様編集画面 700




第 8 図

実行確認画面 800



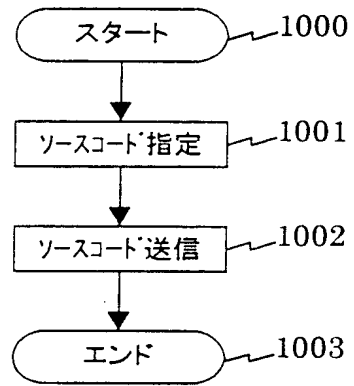
第 9 図

機能仕様管理ファイル 416



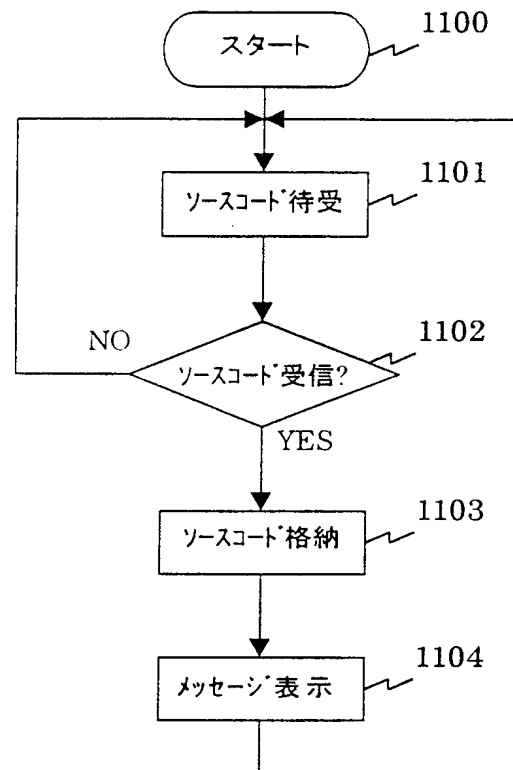
	機能仕様
1	(read /tmp/temp.txt) (write //foo.co.jp:80/tmp/temp.txt)
2	(read //var.com:23/data.doc) (write /tmp/data.doc)
3	(execute /bin/ls -la /etc) (write //foo.co.jp:80/tmp/ls.result)
⋮	⋮

第 10 図



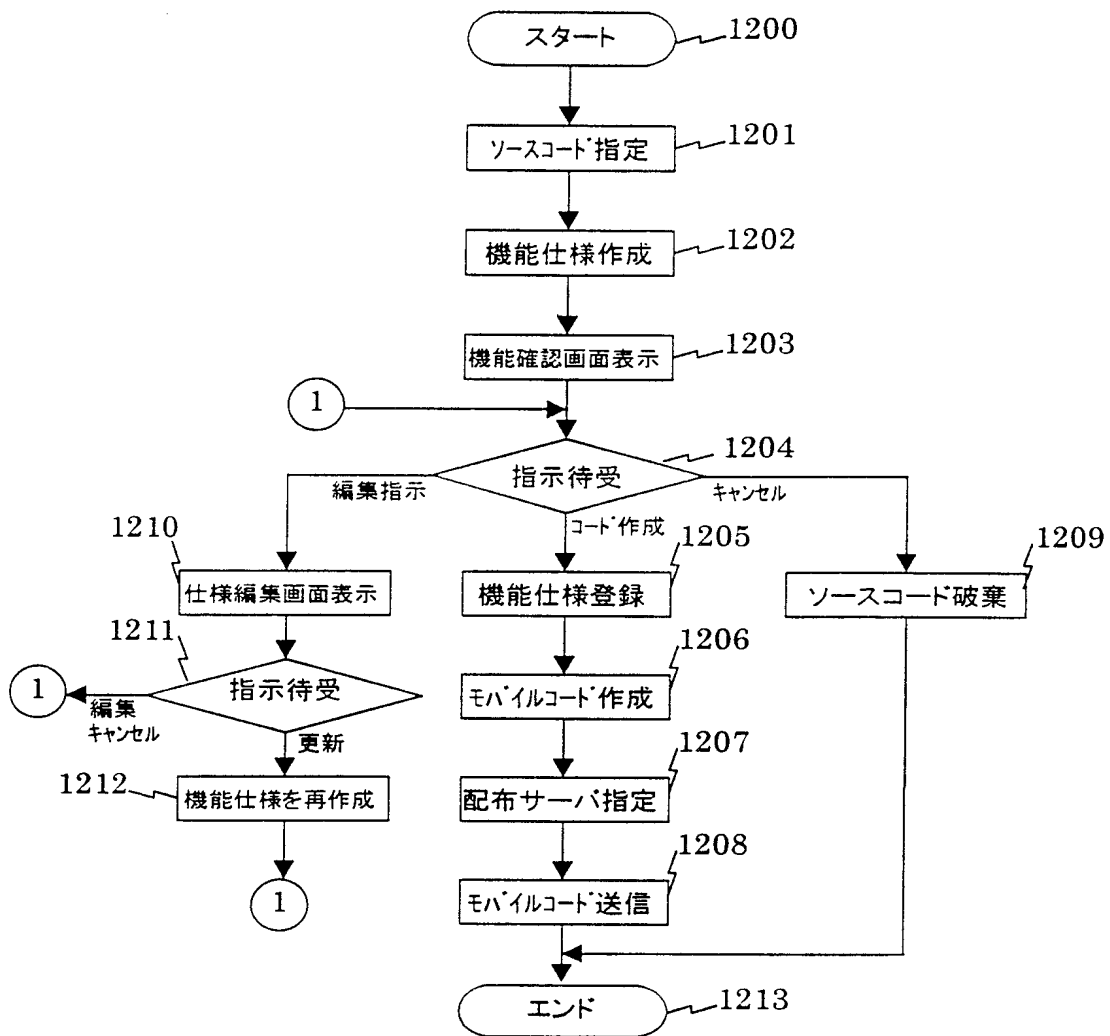
11/20

第 11 図

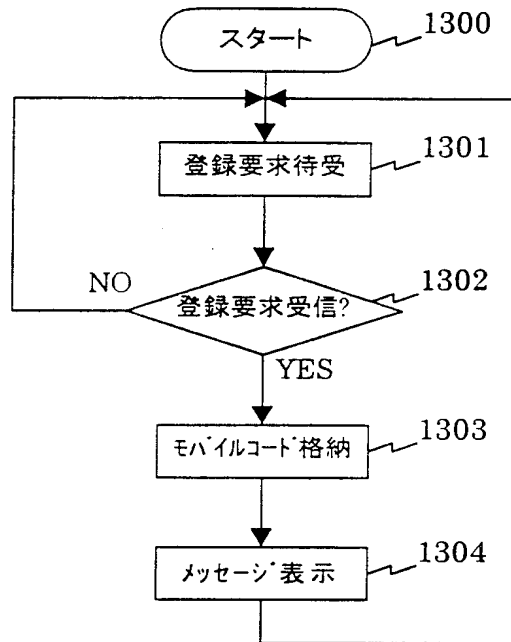


12/20

第 12 図

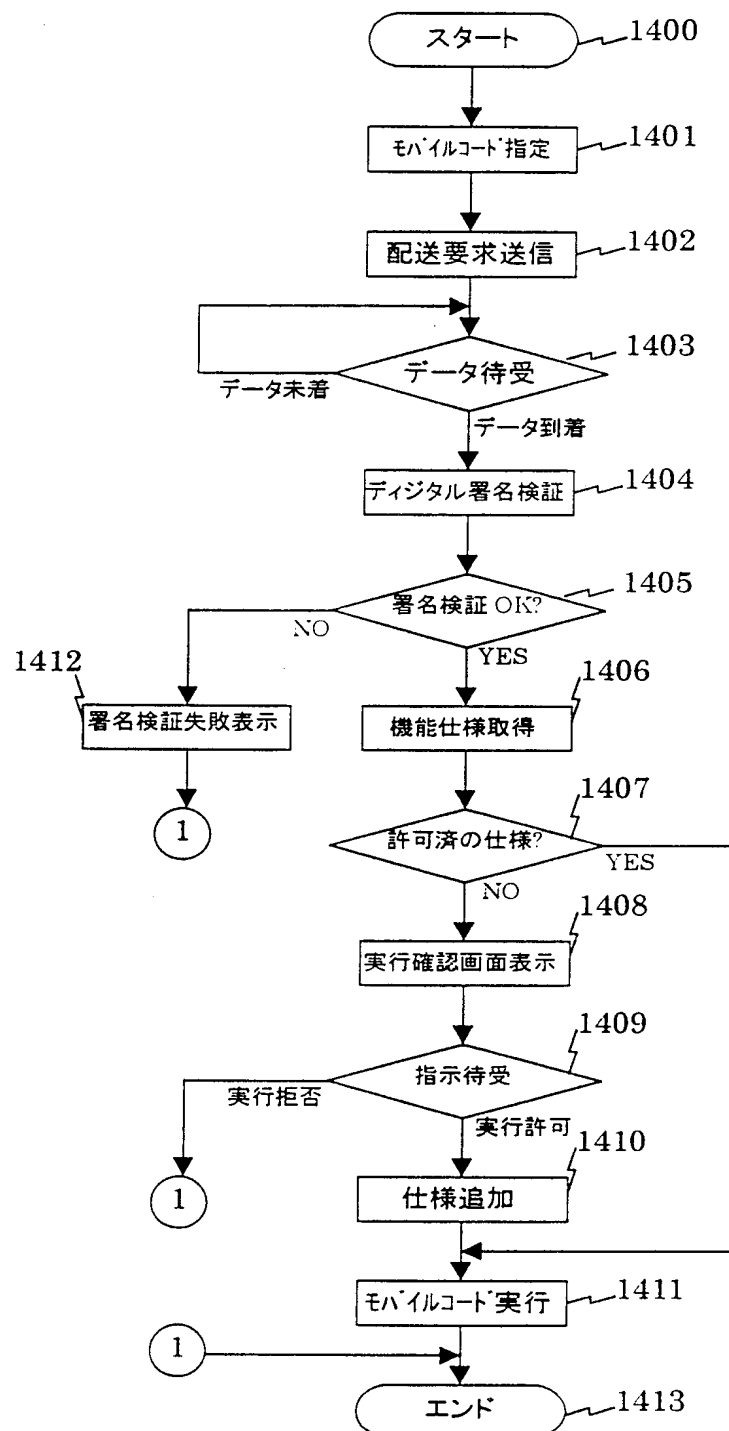


第 13 図

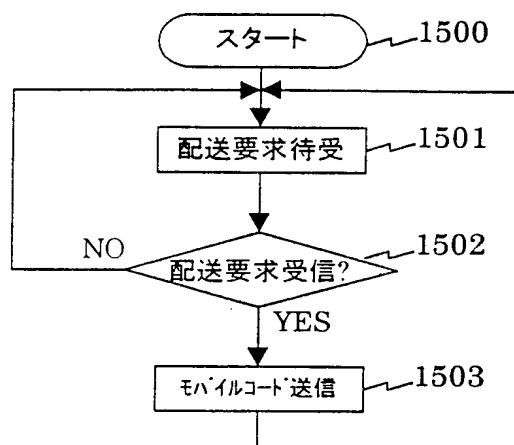


14/20

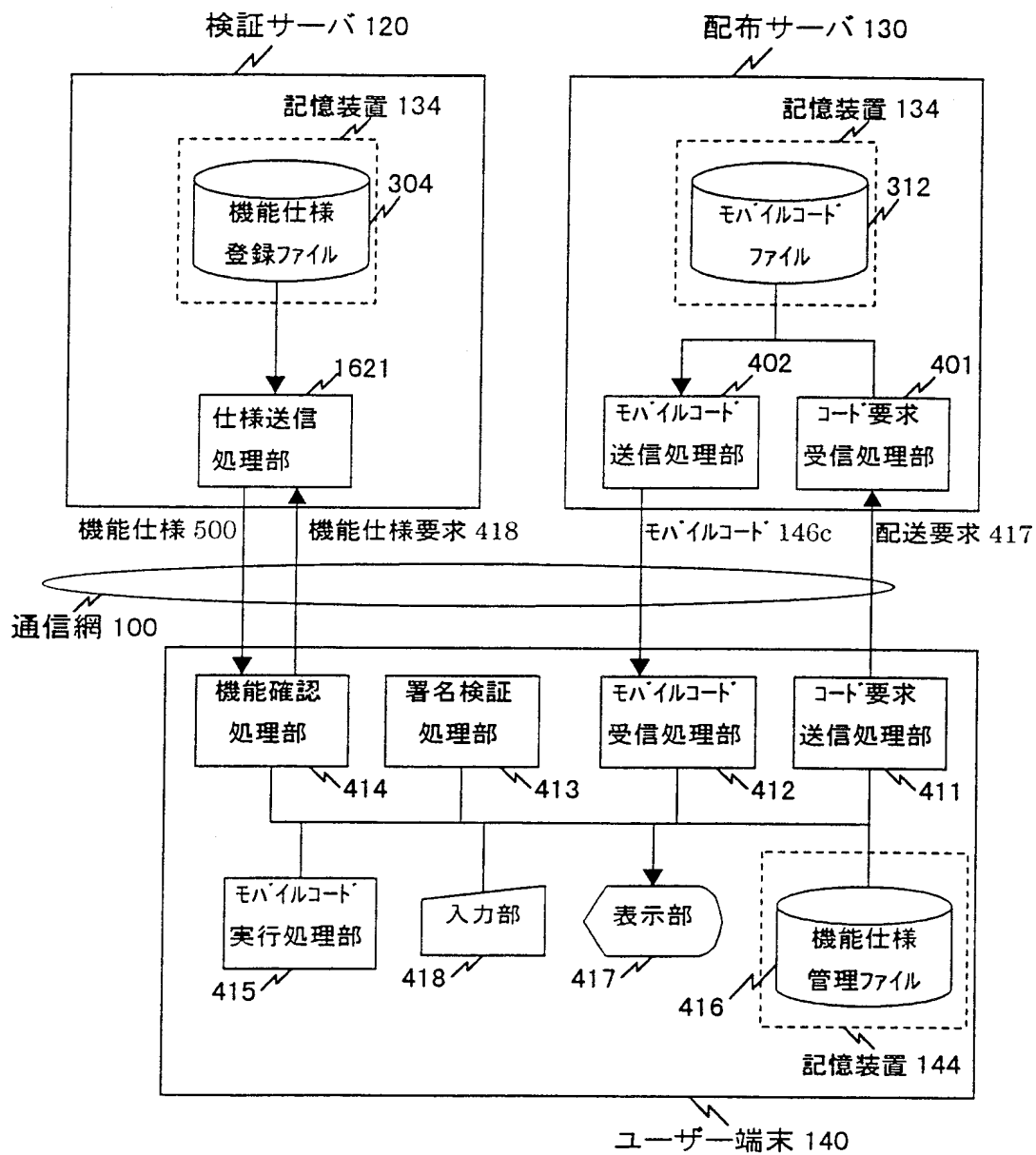
第 14 図



第 15 図

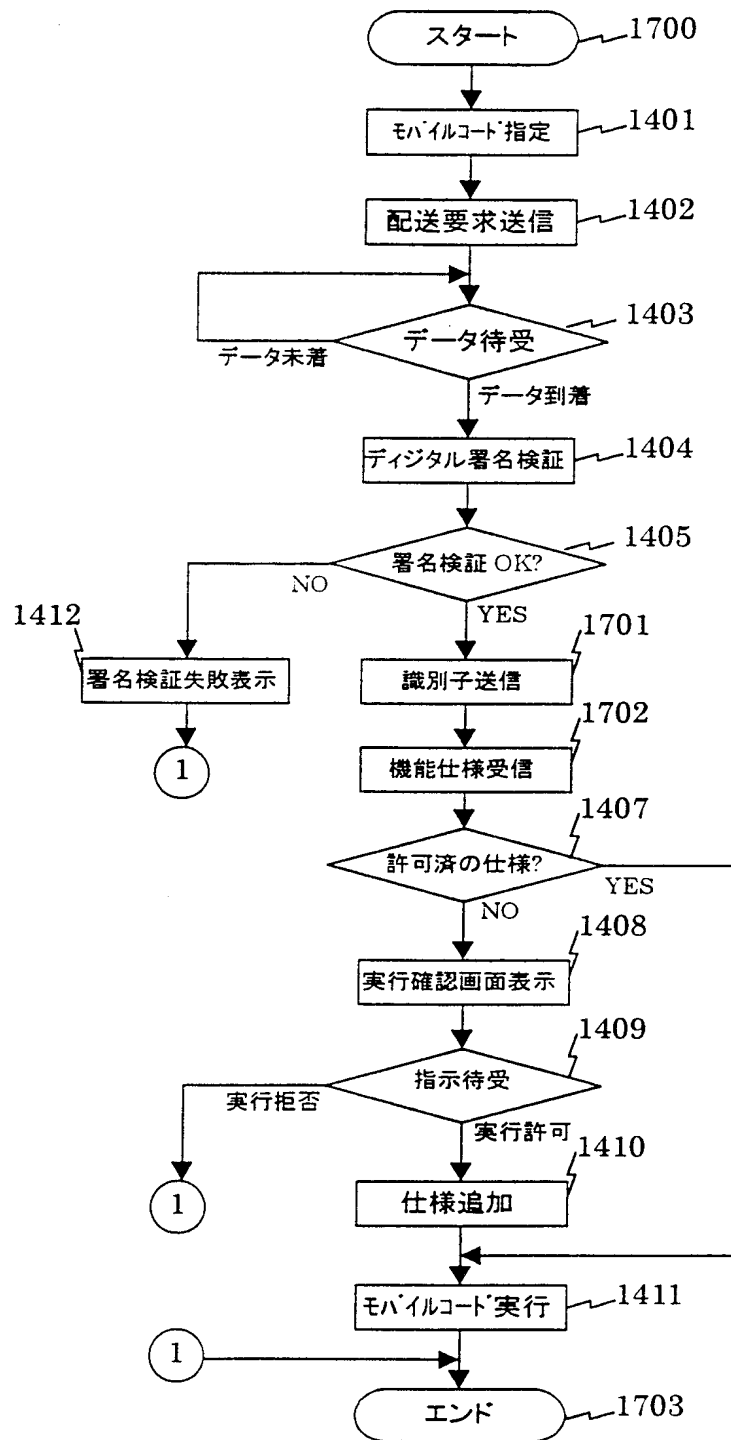


第 16 図

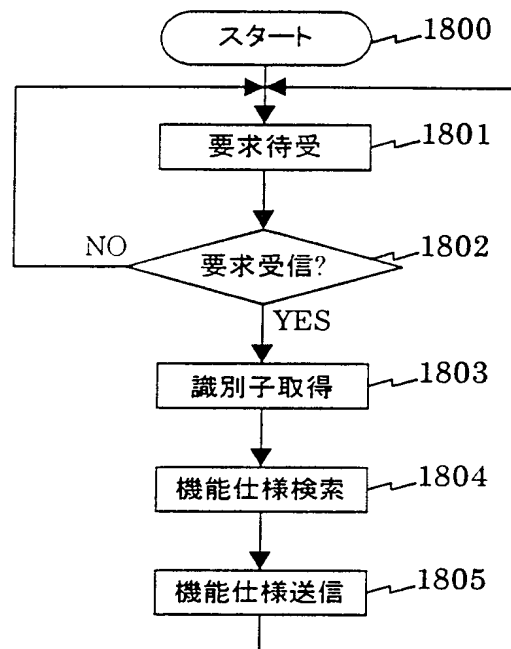


17/20

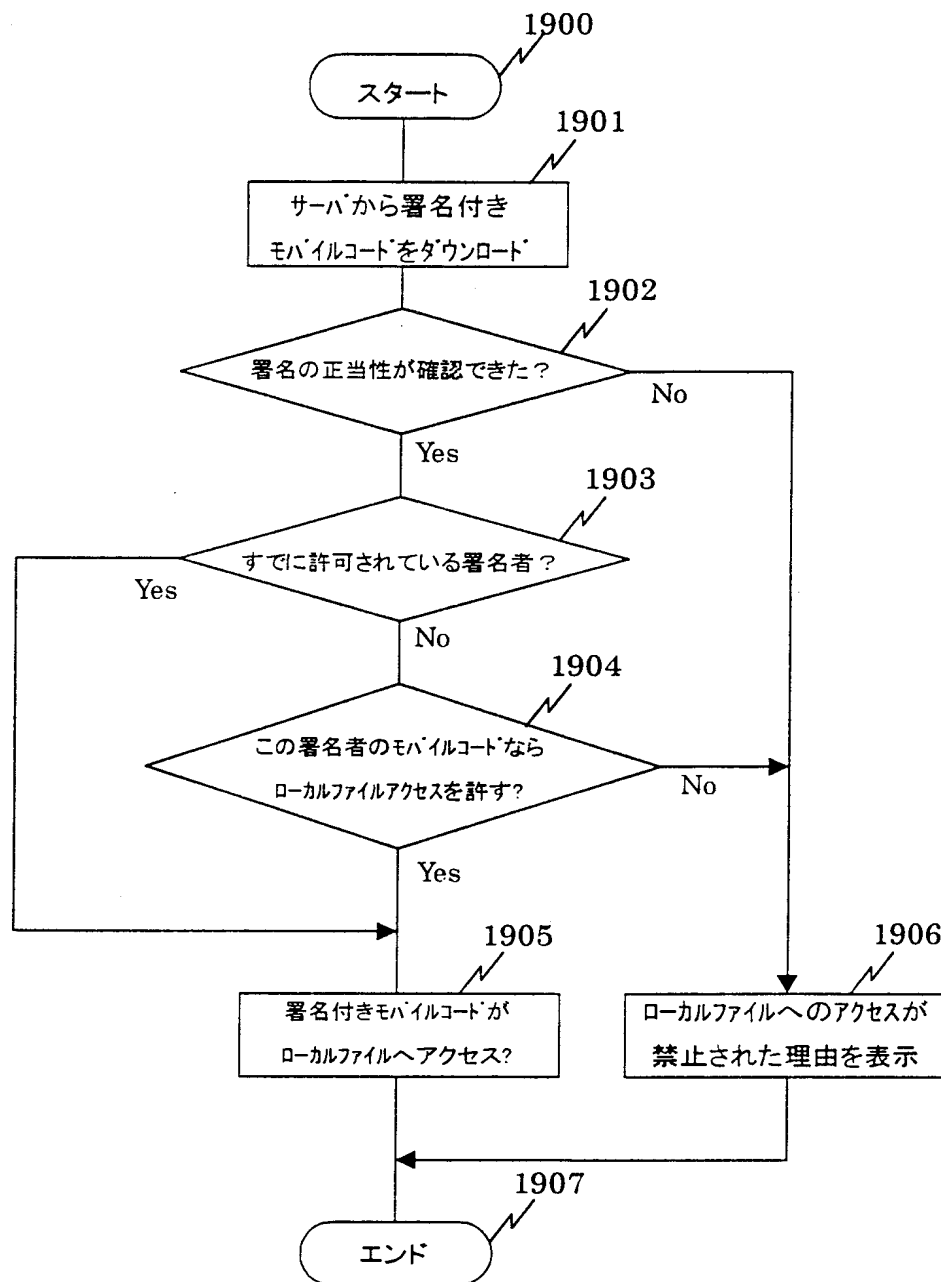
第 17 図



第 18 図



第 19 図



第 20 図

実行確認画面 800

実行確認画面

ファイル ネットワーク その他

2011 読込

2012 /etc/passwd

2012 /etc/hosts

2013 書込

2014 /etc/passwd

2014 /etc/hosts.equiv

2015 実行

2016 /bin/rm -rf /tmp

2016 /sbin/shutdown -h now

機能仕様
表示領域
2010

実行 拒否

実行ボタン 2020 拒否ボタン 2030

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/00084

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁶ G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁶ G06F9/06, G06F9/44, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1971-1996	Toroku Jitsuyo Shinan Koho	1994-1998
Kokai Jitsuyo Shinan Koho	1971-1995	Jitsuyo Shinan Toroku Koho	1996-1997

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Lecture Notes in Computer Science, Vol. 1419 (1998), Gong Li, et al., "Signing, Sealing, and Guarding Java Objects" P.206-216	1-16
A	Shigeru Tago, "JDK1.2 no security kikou o mini tsukeru", Gekkan Java World, Vol. 2, No. 11 (1998-11), P.54-65	1-16
A	Hisashi Kojima, Hiroshi Maruyama, "Java no code shomei model ni kansuru giron", Dai 1 Kai Internet Technology Workshop Rombunshuu (WIT'98) (1998-8)	1-16
A	JP, A, 10-69382 (Sun Micro Systems Inc.), 10 March, 1998 (10. 03. 98) & EP, 778522, A2	1-16
A	JP, A, 9-231068 (Sun Micro Systems Inc.), 5 September, 1997 (05. 09. 97) & EP, 770957, A2	1-16

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
30 April, 1999 (30. 04. 99)Date of mailing of the international search report
18 May, 1999 (18. 05. 99)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/00084

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, A, 10-254783 (Sun Micro Systems Inc.), 25 September, 1998 (25. 09. 98) & EP, 853279, A2	1-16
A	JP, A, 10-83310 (International Business Machines Corp.), 31 March, 1998 (31. 03. 98) & EP, 813132, A2	1-16
A	JP, A, 10-91427 (International Business Machines Corp.), 10 April, 1998 (10. 04. 98) & EP, 813133, A2	1-16

国際調査報告

国際出願番号 PCT/J P 99/00084

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int⁶ G06F9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int⁶ G06F9/06, G06F9/44, G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1971-1996年
 日本国公開実用新案公報 1971-1995年
 日本国実用新案登録公報 1996-1997年
 日本国登録実用新案公報 1994-1998年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	Lecture Notes in Computer Science, Vol. 1419(1998), Gong Li, et al "Signing, Sealing, and Guarding Java Objects" P. 206-216	1-16
A	月刊ジャバワールド, 第2巻, 第11号(1998-11), 多湖 滋 "JDK1.2のセキュリティ機構を身に付ける" P. 54-65	1-16
A	第1回インターネットテクノロジーワークショップ論文集 (WIT'98) (1998-8), 児島尚, 丸山宏, "Javaのコード署名モデルに 関する議論"	1-16

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

30.04.99

国際調査報告の発送日

18.05.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

川崎 優

印

5 B

8944

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, A, 10-69382 (サン・マイクロシステムズ・インコーポレイテッド) 10. 3月. 1998 (10.03.98) & E P, 778522, A2	1-16
A	J P, A, 9-231068 (サン・マイクロシステムズ・インコーポレイテッド) 5. 9月. 1997 (05.09.97) & E P, 770957, A2	1-16
A	J P, A, 10-254783 (サン・マイクロシステムズ・インコーポレイテッド) 25. 9月. 1998 (25.09.98) & E P, 853279, A2	1-16
A	J P, A, 10-83310 (インターナショナル・ビジネス・マシーンズ・コーポレーション) 31. 3月. 1998 (31.03.98) & E P, 813132, A2	1-16
A	J P, A, 10-91427 (インターナショナル・ビジネス・マシーンズ・コーポレーション) 10. 4月. 1998 (10.04.98) & E P, 813133, A2	1-16